FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators with DO-178B

A few more “common sense” tools for your DER toolbox…

(by no means a complete risk or defect management guide)

Risk Indicators

(Do you really have time to monitor even more stuff?)

- Too much to do?
- Too many programs to support?
- Have suppliers that just don’t “get it”?
- Management blaming the DER for missed schedules?
- Tired of convoluted “process” initiatives?

FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators

(Maybe there is a different way for a DER to set priorities…)

- What if you could develop a set of
  simple,
  small,
  meaningful
  indicators to prioritize your activities and your time?
- Sound too much like program management?
- Does it mean that a DER might have to be concerned with ***metrics***?

Risk Indicators

(Required indicators a DER currently uses)

- Risk management, mitigation, and elimination is the cornerstone of current regulatory guidance
- In terms of software, risk management has many facets including
  - risk identification (FHA)
  - risk mitigation effectiveness (SSA)
  - layered verification techniques
  - reviews
  - structural coverage analysis
  - requirements coverage analysis
  - independent oversight
  - mission dependent validation techniques
  - and on, and on, and on

Which, if any, of these are indicators or metrics?

- Given all that, is there anything else we could consider, and if so what are some things we would want to consider?

FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators

(How often does a DER need to look at the required indicators?)

- Does the DER need to look at document(s) more than once?
- If not, how does the DER **know** when to look?
- If not, what can be done to reduce the "paper piles" at the end of the program?
  (ever notice how schedules never allow time for DER review?)
- How can a DER deal with concurrent development programs?
- **Can schedule and "quality" problems impact overall risk associated with a given device?**

Risk Indicators

(Some ideas for your DER toolbox…)

- Tracking "software maturity" and "software completeness" can help prioritize DER activities
  - although it would be nice, the program will often not help us (without encouragement)
  - depending on the organization, programs may actually try and hide the information
- Even without cooperation one can ferret a lot of information out of the problem report/change report process
  - DO-178B can be used as a hammer – it requires PR/CC processes (7.1, 7.2.n*, 11.4, 12.1.5, etc)

** - "It is generally recognized that early implementation of change control assists the control and management of software life cycle process activities."*

FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators

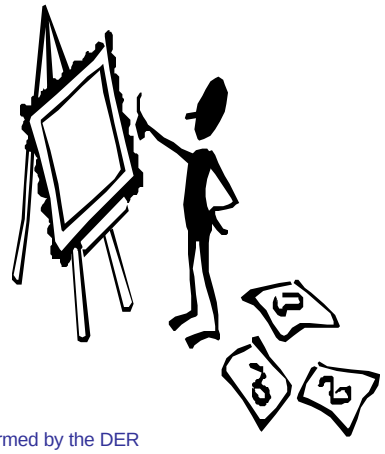
(Setting the groundwork…)

- Besides the obligatory PR/CR processes, what else is needed that ***should*** be a given?
  - Development and verification plans that provide the planned activities and work products (need to use the applicant's terminology)
  - Scope & schedule information
    - » How many system requirements are planned?
    - » How many high-level requirements are planned?
    - » How many low-level requirements are planned?
    - » How many modules do are expected?
    - » On average what is the planned ratio of requirements to requirements based test (RBT) procedures?
    - » What kind of structural coverage is expected from the RBT and how much back-fill is planned?
    - » What is the schedule for completing each activity? Are there meaningful milestones for each major activity?
- This sounds suspiciously like program management but without the info how will you, as a DER, prioritize your work and communicate your plans?

Risk Indicators

(Preparation and assembling the tools…)

- Assuming all of the previous data is available, either build or have the applicant build* a series of simple graphs
- The graphs would have the following data series:
  - a "top line" or **total** planned units
  - a "plan line" that indicates **planned** completion rate
  - an "actual line" that indicates **actual** completion rate
  - a "recovery line" that indicates how much additional work is required to **recover** to the plan line
- In addition to the simple progress charts, several defect charts need to be developed as well



* - All of the subsequent activities will either need to be performed by the DER or by the applicant – there is better buy-in if the applicant observes and records their own trends

FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators

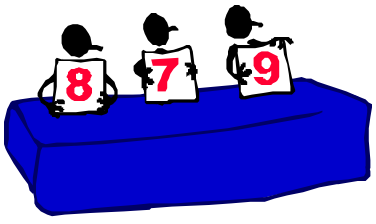
(Preparation and assembling the tools…)

- There are two types of general defects to be concerned with…
  - In-phase defects – defects that are discovered as a result of reviewing the work product as soon as it is completed
    - » e.g., requirements errors found when a requirement thread is reviewed
  - Out-of-phase defects – defects that are discovered when subsequent development or verification tasks are performed
    - » e.g., requirements errors found when an *implemented* requirement thread is tested
- In-phase defects are to be expected and are part of our business (though excessive levels may be cause for further investigation)
- Out-of-phase defects occur, but the goal is to keep the number of out-of-phase defects as small as possible due to the potential for large of number of side effects involved with correcting the original defect

Risk Indicators

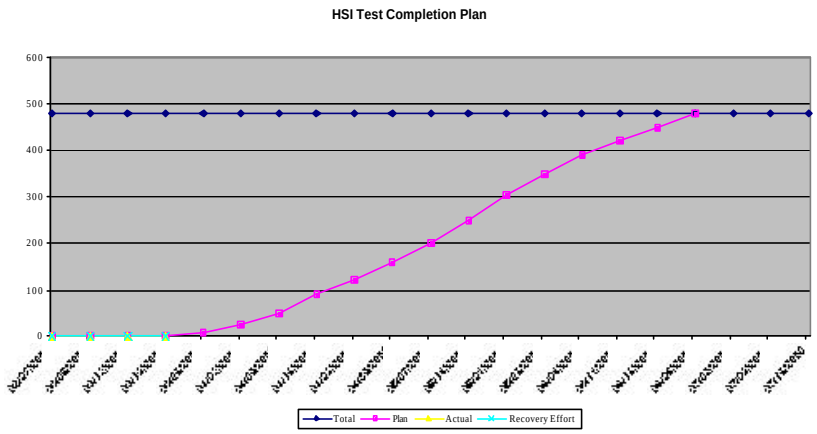
(It is all sounds like common sense, right?)

- How many programs have you worked that could and would provide accurate, graphical indicators for status and defects?
- How many programs have you worked that could give you an accurate picture of total work planned (in terms of either hours or units)?
- If you are working with a supplier, who in your organization has more visibility into actual product issues than you?
- Would your management want to hear your message if you could not get the supplier data you needed to do your job?



FAA National Software Conference
Risk Indicators with DO-178B

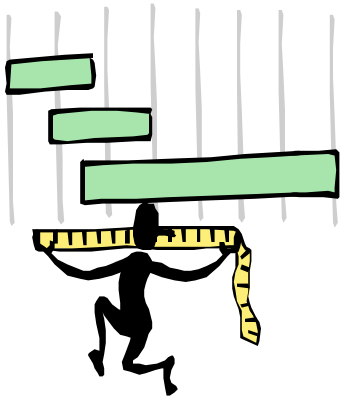
Risk Indicators
(Sample progress indicators)



Are there potential problem(s) from a DER perspective?

Risk Indicators
(Guidelines for progress indicators)

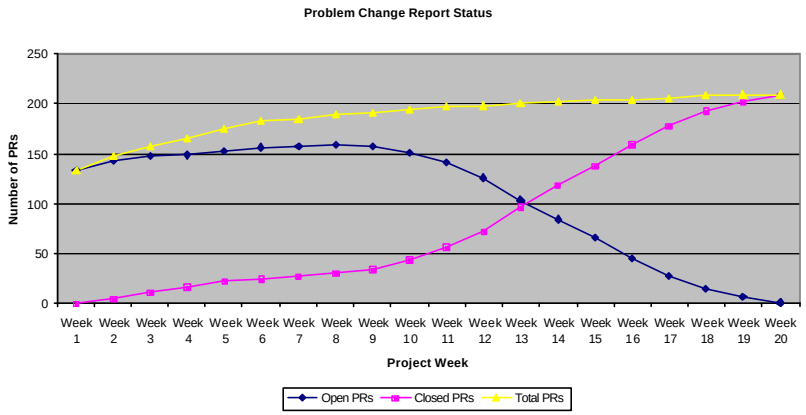
- Need a chart for each major activity
  - System requirements
  - High level requirements
  - Low level requirements
  - Implementation
  - Low level test (structural testing)
  - High level test (RBT)
  - System test
- Be **very clear** with respect to ***when*** credit may be taken
  - Do not count as complete until a review is complete
  - Counting units without a review is a good way to build a large "bow wave" of work
  - If necessary, have the applicant track total units "ready for review" and total units reviewed



Could significantly missing the plan line affect the device risk ?

FAA National Software Conference
Risk Indicators with DO-178B

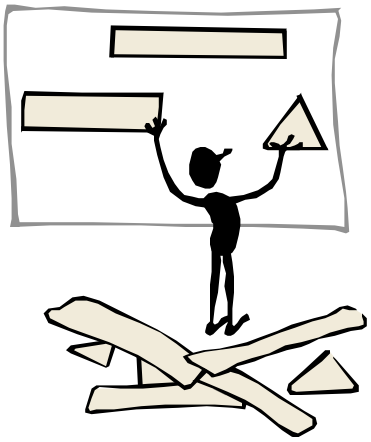
Risk Indicators
(Sample problem and change report indicators)



What can you infer from this graph in terms of maturity?

Risk Indicators
(Guidelines for Problem Report/Change Report indicators)

- What conclusions could be drawn from the previous chart if –
  - there was a high PR/CR generation rate?
    - » unstable requirements
    - » error-prone work artifacts (ineffective reviews?)
    - » untrained staff
    - » high staff turnover
  - the generation rate exceeds the closing rate?
    - » likely schedule slips
    - » "hack" mode
    - » not ready for formal test
  - the closing rate exceeds the generation rate?
    - » probably good – may indicate a level of software maturity/stability
    - » ready for test



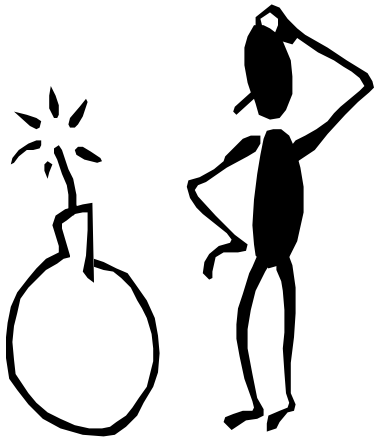
Could high generation rates infer higher product risk?

FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators

(Things look bad – how do can we get somebody's attention?)

- When all else fails, management will always pay attention to dollars…
- One of the major challenges for a DER is identifying a way to raise a flag without being an "alarmist"
  - problems need to be quantified with data
  - when available, use real data
  - when data is not available, make it up
    - » there is a difference between **fiction** and **heuristics**
    - » heuristics are available through both experience and published literature
  - when data is made up, cite your sources, e.g.,
    - » current literature
    - » previous programs
    - » previous supplier's performance



Risk Indicators

(Defect and impact tables – getting management's attention)

	Sys Req	HL Req	LL Req	Code	Unit Test	Int Test	Sys Test	Post Rel
Sys Req	**44**							
HL Req	16	**29**						
LL Req	4	9	**40**					
Code	1	3	13	**69**				
Unit Test	0	2	3	15	**4**			
Int Test	2	1	1	2	2	**16**		
Sys Test	2	2	0	1	1	3	**8**	
Post Rel	1	0	0	0	0	0	0	**8**

	Sys Req	HL Req	LL Req	Code	Unit Test	Int Test	Sys Test	Post Rel
Sys Req								
HL Req	**2**							
LL Req	**4**	**2**						
Code	**8**	**4**	**2**					
Unit Test	**16**	**8**	**4**	**2**				
Int Test	**32**	**16**	**8**	**4**	**2**			
Sys Test	**64**	**32**	**16**	**8**	**4**	**2**		
Post Rel	**128**	**64**	**32**	**16**	**8**	**4**	**2**	

Blue numbers on the diagonal represent defects found "in-phase"

Numbers off the diagonal represent defects found out of phase

Red numbers are impact scale factors for out-of-phase defect resolution

The scale factors will vary, but is safe to say each scale factor is > 1.0X

Most literature suggests at least 2X

FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators

(Combine the defect and impact tables)

	Sys Req	HL Req	LL Req	Code	Unit Test	Int Test	Sys Test	Post Rel
Sys Req	**44**							
HL Req	64	**29**						
LL Req	64	36	**40**					
Code	64	48	52	**69**				
Unit Test	0	128	48	60	**4**			
Int Test	2048	256	64	32	8	**16**		
Sys Test	8192	2048	0	64	16	12	**8**	
Post Rel	16384	0	0	0	0	0	88	**8**
Total	26860	2545	204	225	28	28	96	8

We can debate the scale factors, but the results are sobering – out-of-phase defects are expensive and time consuming

Units on the impact numbers will depend on your approach ($$$ vs. hours)

Risk Indicators

(Caveats and disclaimers)

- The approach presented today has been superficial, but was intended to be practical
  - If the approach is just “common sense”, how come we don’t see it practiced more often?
  - there are many more scientific and esoteric approaches to defects and tracking than those presented today – check them out when you get the time
- Like it or not, DERs involved with SW have to be involved with measures at some level – the single word definition for combined or compound measurements is “metric”
- Metrics do not negate the need for domain knowledge, software engineering skills, and the “dog work” that is involved with being a good DER
- Metrics can be used to prioritize your work
  - if schedules are consistently being missed your “next program” may be further away than you thought
  - if PR/CR rates are high, there is no real need to get too anxious about doing reviews for “score”
  - if there is a high level of out-of-phase work occurring, your review work and/or compliance findings may have to wait a while

Risk Indicators
(Conclusions)

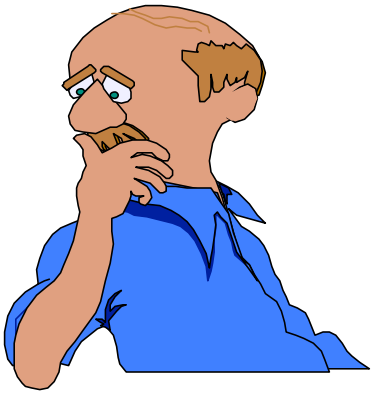
- Metrics are often not collected until there is a crisis
  - it would be easier to mitigate a crisis if we started earlier and had more time to react – metrics can help us do just that
  - work with your supplier to get them started with **meaningful** metrics
    - » with the current emphasis on SEI, ISO, 6Sigma, Spice, etc, etc, there are lots of misguided, worthless metrics being generated
- Good metrics take time
  - be willing to let your supplier's metric approach mature
  - encourage your supplier to kill metrics that are either useless or obsolete
- A small, meaningful set of linear metrics that provide a composite view of the product are better than vague, complex, theoretical measures
- Trends and indications are more important than precision – your reviews and domain knowledge will get at the important areas when the product is ready

All metrics today, and the relationships derived from them, are at best quantified rules of thumb dressed up in statistical finery – they provide guidance. Do not use them as rigid rules.

-Boris Beizer

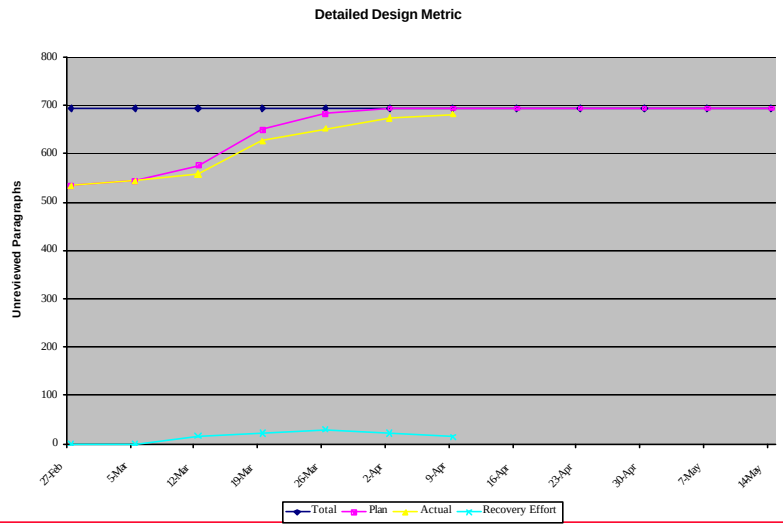
Notable "Quotables" Concerning Measurements

- "Nothing ever happens as quickly as you want."
- "Poor planning on the part of the applicant does not warrant panic on our part."
- Don't go where you have no invitation.



FAA National Software Conference
Risk Indicators with DO-178B

Real Data Wrap-up
Design Data - April 2000

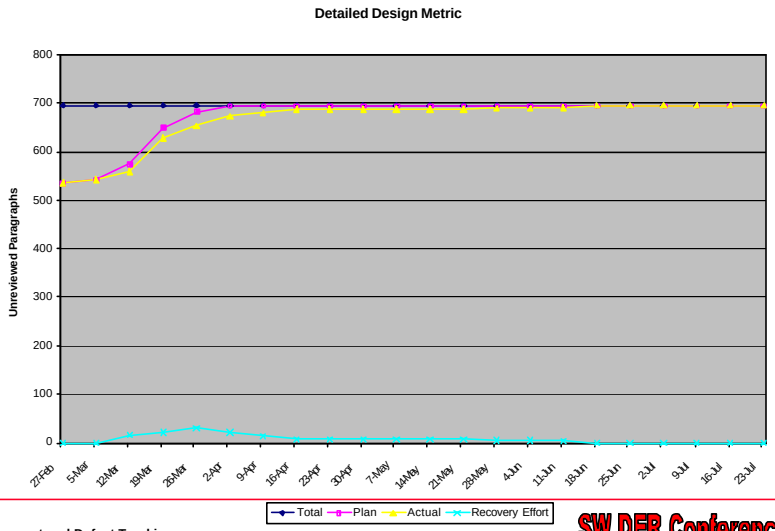


Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

21

SW DER Conference 2000

Real Data Wrap-up
Design Data - August 2000



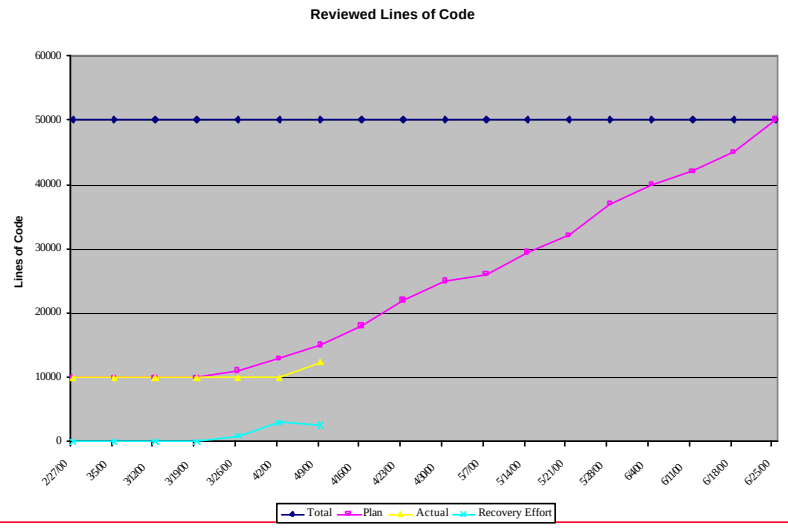
Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

22

SW DER Conference 2000

FAA National Software Conference
Risk Indicators with DO-178B

Real Data Wrap-up
Reviewed Code - April 2000

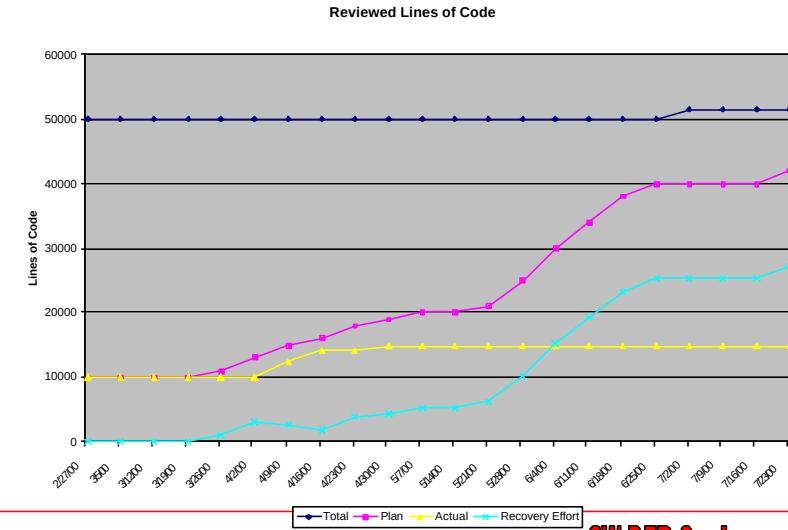


Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

23

SW DER Conference 2000

Real Data Wrap-up
Reviewed Code - August 2000



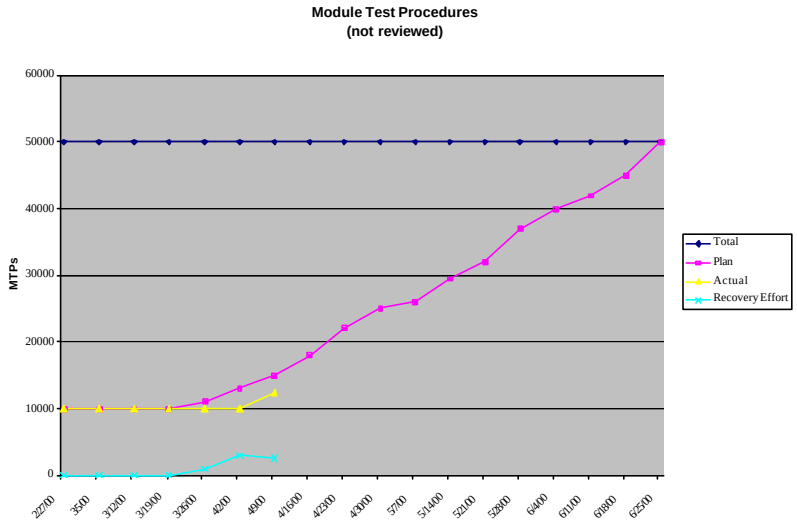
Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

24

SW DER Conference 2000

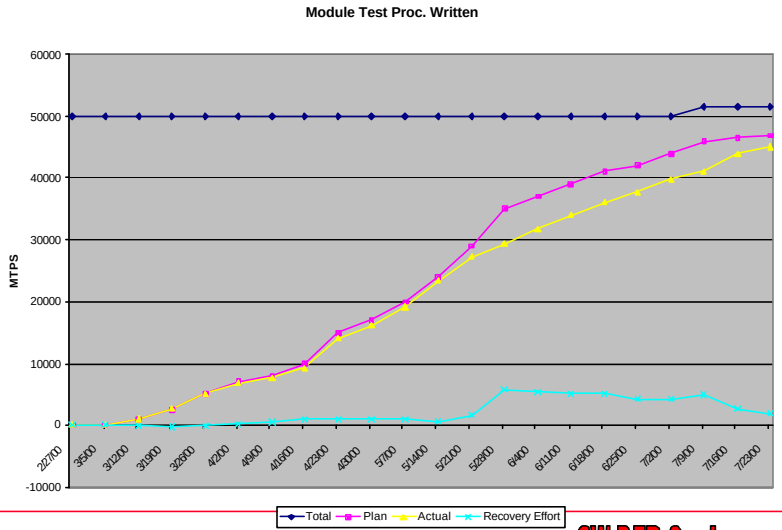
FAA National Software Conference
Risk Indicators with DO-178B

Real Data Wrap-up
MTP Status - April 2000



Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000
25
SW DER Conference 2000

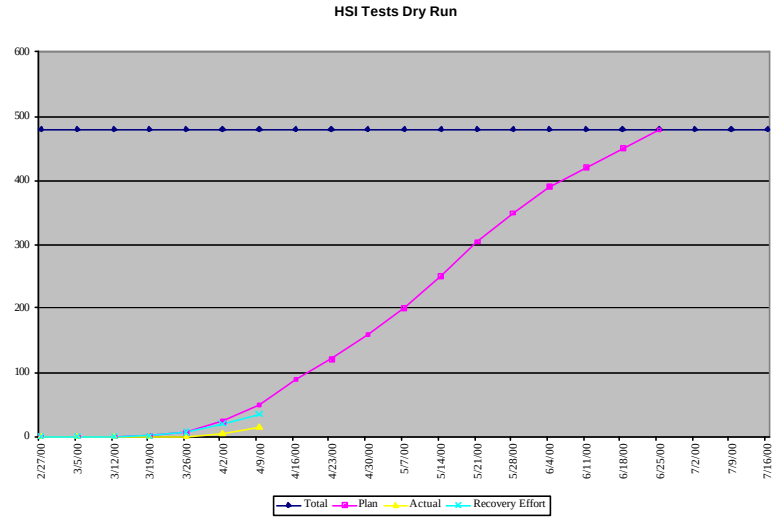
Real Data Wrap-up
MTP Status - August 2000



Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000
26
SW DER Conference 2000

FAA National Software Conference
Risk Indicators with DO-178B

Real Data Wrap-up
HSI Status - April 2000

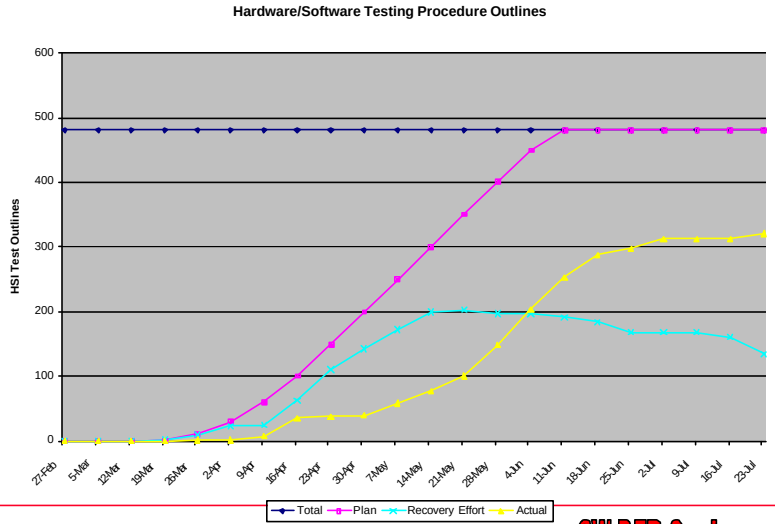


Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

27

SW DER Conference 2000

Real Data Wrap-up
HSI Status - August 2000



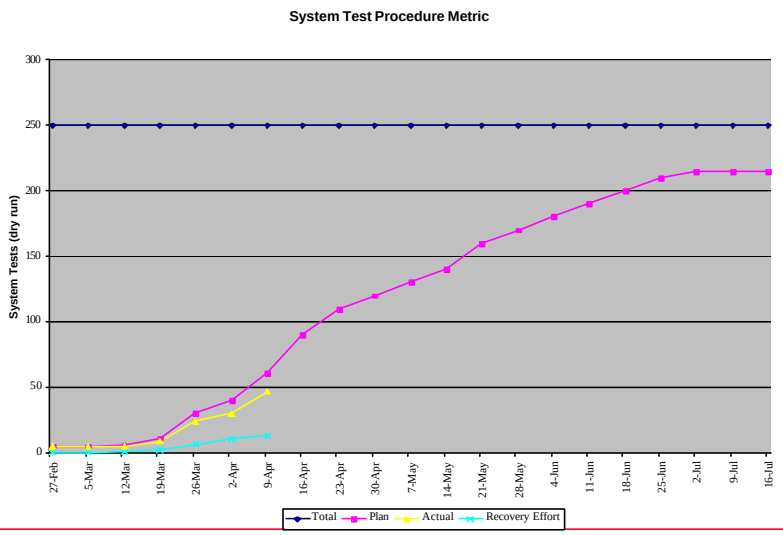
Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

28

SW DER Conference 2000

FAA National Software Conference
Risk Indicators with DO-178B

Real Data Wrap-up
System Test Status - April 2000

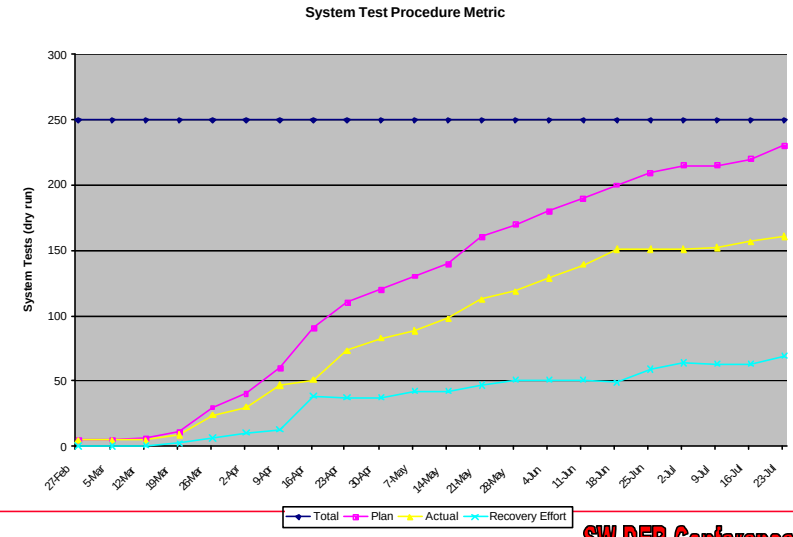


Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

29

SW DER Conference 2000

Real Data Wrap-up
System Test Status - August 2000



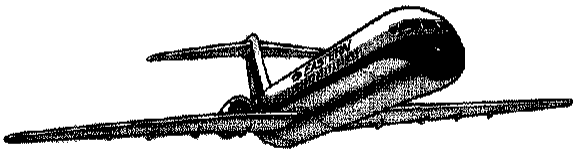
Risk Management and Defect Tracking
© Jeff Knickerbocker, 2000

30

SW DER Conference 2000

FAA National Software Conference
Risk Indicators with DO-178B

Risk Indicators
(Reality Check)

In spite of "way cool, high tech toys" and fancy techniques, it is still all about people!

- COMMUNICATE
  - with the team members
- COMMUNICATE
  - with the supplier
- COMMUNICATE
  - with management
- COMMUNICATE
  - with your ACO